UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/822,542	03/30/2001	Michael S. Ripley	42390P10453	7664

7590 07/06/2005

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Supplemental **Notice of Allowability**	Application No. 09/822,542	Applicant(s) RIPLEY ET AL	
	Examiner Matthew B. Smithers	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an amendment filed December 20, 2004*.

2. ☒ The allowed claim(s) is/are *1-60*.

3. ☒ The drawings filed on *20 March 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with MS. Libby Hope on June 28, 2005.

The application has been amended as follows:

IN THE CLAIMS:

1. (Original) A method comprising:

reading validation data from a validation area (VA) region of a medium having encrypted content;

determining keylng materlal used to decrypt the encrypted content W

deriving the keying material from the validation data: and

using the keying material to decrypt the encrypted content.

2. (Original) The method of claim 1, wherein the keying material is derived from the validation data by using the validation data itself where the validation data comprises the keying material.

3. (Original) The method of claim 1, wherein the keying material is derived from the validation data by using the validation itself where the validation data is a copy of the keying material that is written to the non-VA region of the medium.

4. (Original) The method of claim 3, wherein the medium uses CPPM (Content Protection For Prerecorded Media) format to protect the content. and:

the keying material comprises an album identifier that is written to the non-VA region of the medium; and

the validation data comprises a copy of the album identifier.

5. (Original) The method of claim 1, wherein the keying material is derived from the validation data by converting the validation data in the VA region into the keying material in the non-VA region.

6. (Original) The method of claim 5, wherein the converting the validation data into the keying material comprises using a function for converting the validation data into the keying material, the reverse function having been used to create the validation data from the keying material.

7. (Original) The method of claim 6, wherein the medium uses CSS (Content Scramble System) format to protect the content, and:

the keying material comprises Secure Disc Key Data that is written to the non-VA region of the medium; and

the valldation data comprises a cryptographic function on the Secure Disc Key Data.

8. (Original) The method of claim 6. wherein decrypting the encrypted content comprises using the keying material to form a cryptographic key to decrypt the encrypted content.

9. (Original) The method of claim 6, wherein the medium comprises a DVD (Digital Versatile Disc), and the VA comprises a burst cutting area of the DVD.

10. (Original) A method comprising:

determining if a medium havlng encrypted content is a Validated Medium by determining if validatlon data exists in a validation area (VA) region of the medium;

if the medium is a Validated Medium, determining keying material used to decrypt the encrypted content by deriving the keying material from the validation data; and validating the keying material.

11. (Original) The method of claim 10, wherein said determining If the validation data exists in the VA region comprises determining if a trigger has been set.

12. (Original) The method of claim 11, wherein said determining if the trigger has been set comprises determining if the most significant bit of the keying material is set to 1 .

13. (Original) The method of claim 10, wherein the keying material is derived from the validation data by using the validation data itself where the validation data comprises the keying material.

14. (Original) The method of claim 10, wherein the keying material is derived from the validation data by using the validation itself where the validation data is a copy of the keying material that is written to the non-VA region of

the medium.

15. (Original) The method of claim 10, wherein the keying material is derived from the validation data by converting the validation data In the VA region into the keying material in the non-VA region.

16. (Original) The method of claim 10, wherein the medium comprises a DVD (Digital Versatile Disc), and the VA comprises a burst cutting area of the DVD.

17. (Original) A method comprising:

determining if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium, the medium additionally having keying material written to a non-VA region of the medium;

if the medium is a Validated Medium, determining if the validation data and the keying material correspond; and

if the validation data and the keying material correspond, using the keying material in the non-VA region to decrypt the encrypted content.

18. (Original) The method of claim 17, wherein said determining if the medium is a Validated Medium comprises determining if a trigger has been set.

19. (Original) The method of claim 18, wherein said determining if the trigger has been set comprises determining if the most significant bit of the keying material is set to 1.

20. (Original) The method of claim 17, wherein the medium comprises a DVD-

ROM (Digital Video Disc - Read Only Memory).

21. (Original) The method of claim 17 wherein said determining if the validation data and the keying material correspond comprises determining if the validation data and the keying material match.

22. (Original) The method of claim 21, wherein the medium uses CPPQ (Content Protection For Prerecorded Media) format to protect the content, and:

the keying material comprises an album identifier that is written to the non-VA region of the medium; and

the validation data comprises a copy of the album identifier.

23. (Original) The method of claim 17, wherein said determining if the validation data and the keying material correspond comprises determining if a cryptographic function on the keying material matches the validation data.

24. (Original) The method of claim 23, wherein the medium uses CSS (Content Scramble System) format to protect the content, and:

the keying material comprises Secure Disc Key Data that is written to the non-VA region of the medium; and

the validation data comprises a cryptographic function on the Secure Disc Key Data.

25. (Original) The method of claim 17, wherein the medium comprises a DVD (Digital Versatile Disc), and the VA comprises a burst cutting area of the DVD.

26. (Original) A method comprising:

determining if a medium having encrypted content is a Validated Medium by determining if validation data exists In a validation area (VA) region of the medium; and

if the medium is a Validated Medium, then performing one of the following;

determining keying material used to decrypt the encrypted content by deriving the keying material from the validation data, and then validating the keying material; and

determining if the validation data and the keying material correspond, and validating the keying material if the validation data corresponds to the keying material.

27. (Original) The method of claim 26. wherein the keying material is derived from the validation data by using the validation data itself where the validation data comprises the keying material.

28. (Original) The method of claim 26, wherein the keying material is derived from the validation data by using the validation itself when the validation data is a copy of the keying material that is written to the non-VA region of the medium.

29. (Original) The method of claim 26, wherein the keying material is derived from the validation data by converting the validation data in the VA region into the keying material in the non-VA region.

30. (Original) The method of claim 26, wherein the medium comprises a DVD-

ROM (Digital Video Disc - Read Only Memory).

31. (Original) The method of claim 26, wherein the VA comprises a burst cutting area.

32. (Original) A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

determine if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium; and

if the medium is a Validated Medium, then perform one of the following:

determine keying material used to decrypt the encrypted content by deriving the keying material from the Validation data, and then validate the keying material; and

determine if the validation data and the keying material correspond, and validate the keying material if the validation data corresponds to the keying material.

33. (Original) The machine-readable medium of claim 32, wherein the encrypted content is protected using CPPM (Content Protection for Prerecorded Media) format, and the keying material comprises an album identifier, and the validation data comprises a copy of the album identifier.

34. (Original) The machine-readable medium of claim 32, wherein the content

is protected by CSS (Content Scrambling System), and:

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

35. (Original) An apparatus comprising:

at least one processor; and

a machine-readable medium having instructions encoded thereon, which when executed by the processor, are capable of directing the processor to:

determine if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium; and

if the medium is a Validated Medium, then perform one of the following;

determine keying material used to decrypt the encrypted content by deriving the keying material from the validation data, and then validate the keying material;

and

determine if the validation data and the keying material correspond, and validate the keying material if the validation data corresponds to the keying material.

36. (Original) The apparatus of claim 35, wherein the encrypted content is protected using CPPM (Content Protection for Prerecorded Media) format,

and the keying material comprises an album identifier, and the validation data comprises a copy of the album identifier.

37. (Original) The apparatus of claim 35, wherein the content is protected by CSS (Content Scrambling System), and;

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

38. (Original) An apparatus comprising;

means for determining if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium; and

the medium is a Validated Medium, then means for performing one of the following:

determining keying material used to decrypt the encrypted content by deriving the keying material from the validation data, and then validating the keying material; and

determining if the validation data and the keying material correspond, and validating the keying material if the validation data corresponds to the keying material.

39. (Original) The apparatus of claim 38, wherein the encrypted content is protected using CPPM (Content Protection for Prerecorded Media) format, and the keying material comprises an album identifier, and the validation

data comprises a copy of the album identifier.

40. (Original) The apparatus of claim 38, wherein the content is protected by GSS (Content Scrambling System), and;

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

41. (Original) An apparatus comprising:

encrypted content; and

keying material; and

validation data written to a validation area (VA) region of the medium, the validation data being used to validate the authenticity of the keying material.

42. (Original) The apparatus of claim 41, wherein the encrypted content uses Content Protection For Prerecorded Media (CPPM) format, and the validation data comprises an album identifier that is used to form a cryptographic key for decrypting the content.

43. (Original) The apparatus of claim 41, wherein the keying material is written to a non-VA region of the medium.

44. (Original) The apparatus of claim 41, wherein the apparatus comprises a DVD-ROM (Digital Video Disc - Read Only Memory).

45. (Original) The method of claim 41, wherein the VA comprises a burst cutting area.

46. (Original) An apparatus, comprising:

a first module to determine if validation data exists in a validation area (VA) region of a medium, the medium having keying material for decrypting encrypted content on the medium, and the validation data being used to validate the authenticity of the keying material; and

a second module to process the medium, if validation data exists in the VA region, by performing one of the following:

using keying material derived from the VA region of the medium to decrypt the encrypted content and

finding correspondence between the validation data and the keying material, and if correspondence is found, using the keying material to decrypt the encrypted content.

47. (Original) The apparatus of claim 46, wherein the first module determines if validation data exist in a VA region of the medium by determining if a trigger is set.

48. (Original) The apparatus of claim 47, wherein the trigger is set if the most significant bit of the keying material is set to 1.

49. (Original) The apparatus of claim 46, wherein the validation data corresponds to the keying material if the keying material matches the validation data.

50. (Currently Amended) A system comprising:

a medium having:

encrypted content;

keying material; and

validation data written to a VA region of the medium[.]

a device coupled to the medium to play the encrypted content by performing one of the following:

using the keying material derived from the VA region of the medium to decrypt the encrypted content; and

determining if the validation data corresponds to the keying material and if the validation data corresponds to the keying material, then using the keying material to decrypt the encrypted content.

51. (Original) The system of claim 50, wherein the content is protected by CPPM (Content Protection For Prerecorded Media), and the keying material has an album identifier that is used to form a cryptographic key for decrypting the content.

52. (Original) The system of claim 50, wherein the content is protected by CSS (Content Scrambling System), and;

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

53. (Original) A system comprising:

a medium having:

encrypted content; and

keying material; and

a device coupled to the medium to decrypt the encrypted content if the medium is a Validated Medium, and the authenticity of the keying material is validated.

54. (Original) The system of claim 53, wherein the authenticity of the keying material is validated by one of the following:

using the keying material derived from the VA region of the medium; and

determining that the validation data corresponds to the keying material.

55. (Original) The system of claim 54, wherein the validation data corresponds to the keying material if the keying material matches the validation data.

56. (Original) The system of claim 54, wherein the validation data corresponds to the keying material if a function of the keying material matches the validation data.

57. (Original) The system of claim 53, wherein the medium comprises a DVD-ROM (Digital Video Disc - Read Only Memory).

58. (Original) The method of claim 63, wherein the VA comprises a burst cutting area.

59. (Original) The system of claim 53, wherein said determining if the validation data exists in the VA region comprises determining if a trigger

60. (Original) The system of claim 59, wherein said determining if the trigger

has been set comprises determining if the most significant bit of the keying material is set to 1.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137

***